CLAIMS

1.   A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for:

generating a plurality of keys in response to a received challenge;

generating an authentication signal based on a received signal and a first key from the plurality of keys, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit; and

transmitting the authentication signal to the communications system via the communications unit.

2.   The processor of 1, wherein the authentication signal is generated by a hash function.

3.   The processor of 2, wherein the hash function is the Secure Hash Algorithm (SHA-1).

4.   The processor of 1, wherein the authentication signal is generated by an encryption algorithm.

5.   The processor of 4, wherein the encryption algorithm is the Data Encryption Standard (DES).

6. A subscriber identification module, comprising:

2 a key generation element; and

a signature generator configured to receive a secret key from the key

4 generation element and information from a mobile unit, and further configured to output a signature to the mobile unit.

7. The key generation element of Claim 6, comprising:

2 a memory; and

a processor configured to execute a set of instructions stored in the

4 memory, wherein the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys.

8. The processor of Claim 7, wherein the cryptographic transformation is

2 performed using a permanent key.

9. The signature generator of Claim 6, comprising:

2 a memory; and

a processor configured to execute a set of instructions stored in the

4 memory, wherein the set of instructions performs a cryptographic transformation upon the information from the mobile unit by using the secret key, wherein the

6 signature results from the cryptographic transformation.

10. An apparatus for providing secure local authentication of a subscriber in a

2 communication system, comprising a subscriber identification module configured to interact with a communications unit, wherein the subscriber identification

4 module comprises:

a key generator for generating a plurality of keys from a received

6 value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least

8   one secret key from the plurality of keys is not delivered to the communications unit; and

10   a signature generator for generating an authorization signal from both the at least one secret key and from an authorization message,

12   wherein the authorization message is generated by the communications unit using the at least one communication key.

11.   The subscriber identification module of Claim 10, wherein the subscriber

2   identification module is configured to be inserted into the communications unit.

12.   The subscriber identification module of Claim 10, wherein the signature

2   generator generates the authorization signal by using a hash function.

13.   The subscriber identification module of Claim 10, wherein the signature

2   generator generates the authorization signal by using the Data Encryption Standard (DES).

14.   The subscriber identification module of Claim 10, wherein the at least one

2   communication key comprises an integrity key.

15.   The subscriber identification module of 12, wherein the hash function is

2   SHA-1.

16.   A method for providing authentication of a subscriber using a subscriber

2   identification device, comprising:

       generating a plurality of keys;

4   transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification

6   device and holding private at least one key from the plurality of keys;

generating a signature at the communications device using both the at

8   least one key transmitted to the communications device and a transmission message;

10   transmitting the signature to the subscriber identification device;

receiving the signature at the subscriber identification device;

12   generating a primary signature from the received signature; and

conveying the primary signature to a communications system.

17.   The method of Claim 16, wherein the generating of the signature signal is

2   performed using a nonreversible operation.

18.   The method of Claim 16, wherein the generating of the signature signal is

2   performed using DES.

19.   The method of Claim 16, wherein the generating of the signature signal is

2   performed using a hash function.

20.   The method of Claim 19, wherein the hash function is SHA-1.

21.   A method for providing authentication of a subscriber using a subscriber

2   identification device, comprising:

generating a plurality of keys;

4   transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification

6   device and holding private at least one key from the plurality of keys;

assigning a weight to the transmission message at the communications

8   device in accordance with a relative importance of the transmission message;

generating a signature at the communications device using both the at

10   least one key transmitted to the communications device and the transmission message;

12   transmitting the signature to a communications system if the assigned weight to the transmission message indicates that the transmission message is

14   unimportant; and

transmitting the signature to the subscriber identification device if the

16   assigned weight to the transmission message indicates that the transmission message is important, whereupon the subscriber identification device generates

18   a primary signature from the received signature signal, and then conveys the primary signature to a communications system.

20